Las presentes obligaciones se decriben en relación al tratamiento de datos personales, además de las previstas en el artículo 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Difundir al interior de CENDI del Municipio de Tlajomulco de Zúñiga el aviso de privacidad y el documento de seguridad.
2) Revisión física anual a las diversas áreas de CENDI del municipio de Tlajomulco de Zúñiga, Jalisco sobre el tratamiento de datos personales y la implementación de medidas de seguridad.
3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.
4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

ANÁLISIS DE RIESGOS:

Con base a las circunstancias físicas, humanas y generales, en las que este sujeto obligado trata datos personales, se han identificado los siguientes riesgos posibles:

Eliminados 15 renglones, información reservada, artículo 17.1 fracción I inciso A) de la LTAIPEJM, su publicación podría poner en riesgo al CENDI Tlajomulco.

especialidades.
6.- La falta de control preciso sobre las fojas que integran los expedientes de las y los beneficiarios en las diversas áreas que generan expedientes.
7.- La falta de impresión de bases de datos que contienen datos personales.
8.- La falta de mecanismos de resguardo de la información generada a través de medios electrónicos.
9.- Falta de extintores en el área de archivo de concentración de CENDI Tlajomulco.
10.- Filtración de húmedad o aire en el área de archivo de concentración de CENDI Tlajomulco

En virtud de lo antes referido, es preciso realizar el siguiente análisis de riesgos, amenazas y posibles vulneraciones.

Origen de la amenaza	Causa	Posibles consecuencias
Eliminada tabla, información reservada, artículo 17.1 fracción I inciso A) de la LTAIPEJM, su publicación podría poner en riesgo al CENDI Tlajomulco.		

	especialidades.	
Área de archivo de concentración.	Falta de extintores en el área de archivo de concentración de CENDI Tlajomulco.	Pérdida parcial o total de documentos que contengan datos personales en caso de incendio.
Área de archivo de concentración.	Filtración de humedad o aire en el área de	Pérdida parcial o total de documentos que

Eliminada tabla, información reservada, artículo 17.1 fracción I inciso A) de la LTAIPEJM, su publicación podría poner en riesgo al CENDI Tlajomulco.

Cabe señalar que a la fecha de creación del presente documento no se han identificado o reportado vulneraciones desde las áreas generadoras de información de CENDI del Municipio de Tlajomulco de Zúñiga, Jalisco

ANÁLISIS DE BRECHA:

Con base al diagnóstico realizado a las diversas áreas de CENDI el Municipio de Tlajomulco de Zúñiga, asi como del análisis de riesgos y vulneraciones en las áreas que generan información, es procedente efectuar el análisis de brecha, puntualizando que las medidas de seguridad existentes son las siguientes:

MEDIDAS DE SEGURIDAD ADMINISTRATIVA

POLÍTICA DE SEGURIDAD	Eliminados 13 renglones, información reservada, artículo 17.1 fracción I inciso A) de la LTAIPEJM, su publicación podría poner en riesgo al CENDI Tlajomulco.

	derechos de imagen firmada por las madres, padres o tutores de las y los beneficiarios.
Cumplimiento de la Normatividad	Se encuentran adoptando medidas de conformidad a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Municipio de Tlajomulco de Zúñiga, Jalisco y la LTAIPEJM.
Organización de la seguridad de la Información	Eliminados 7 renglones, información reservada, artículo 17.1 fracción I inciso A) de la LTAIPEJM, su publicación podría poner en riesgo al CENDI Tlajomulco
Clasificación y control de activos	Se llevan a cabo controles de inventarios de documentación que contiene datos personales, identificando bases de datos, con la finalidad de ajustarlo a la Ley General de Archivos.
Seguridad Relacionada con recursos humanos	Mediante capacitación impartida por la Dirección De Archivo Municipal en donde se dieron a conocer los alcances jurídicos del manejo de archivos, asi como la orientación de la Unidad de Transparencia respecto a la protección de los datos personales.
Administración de Incidentes	Se adopta con el presente documento de seguridad, mediante la implementación de formatos de incidencias y vulneraciones, descritos como anexo 1 y 2.
Términos y condiciones de empleo	Las y los funcionarios públicos del CENDI del municipio de Tlajomulco de Zúñiga, como parte de su obligación contractual acuerdan y firman los términos y condiciones en su contrato de empleo, el cual indica su responsabilidad respecto a la seguridad de la información.

MEDIDAS DE SEGURIDAD FÍSICAS:

Medidas de seguridad físicas y ambiental	Eliminados 19 renglones, información reservada, artículo 17.1 fracción I inciso A) de la LTAIPEJM, su publicación podría poner en riesgo al CENDI Tlajomulco.

	administrativa, cuyo resguardo se lleva a cabo mediante libreros con cerraduras. Al ingreso del área se encuentra un señalamiento de solo personal autorizado. Asimismo todas las áreas, con excepción de TICS, cuentan con archiveros para llevar a cabo el resguardo de archivos que son considerados "de trámite". Los equipos de cómputo se encuentran sobre escritorios, para efecto de prevenir alguna pérdida de información que sobrevenga de fenómenos meteorológicos.
Seguridad Técnica	Se cuentan con contraseñas de acceso en algunos de los equipos electrónicos, antivirus y para el área de dirección general y administrativa con no break para resguardar la información y proceder al guardado seguro en caso de cese de energía eléctrica.
Control de Acceso	[redacted] A) de la LTAIPEJM, su publicación podría poner en riesgo al CENDI Tlajomulco. imparten terapias mantiene listas de asistencia.

MEDIDAS DE SEGURIDAD PARA TRANSFERENCIAS

Interinstitucionales: Transferencias al interior del sujeto obligado, entidades federativas, otros municipios, otros sujetos obligados. Con entes privados, organizaciones civiles, públicas u otros sujetos obligados Internacionales	1) Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean. 2) El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios. 3) El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces. 4) El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento. 5) El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda. 6) El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales en tratándose de procedimientos de derecho ARCO.
Transferencia a terceros.	1) El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento. 2) En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

MEDIDAS DE SEGURIDAD EN CASO DE VULNERACIONES A LA SEGURIDAD:

Plan de respuesta:

2) Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
3) En caso de que la vulneración fuera resultado de la comisión de un delito, realizar las denuncias correspondientes.
4) Llenado del formato DSA (Anexo 1), por parte de la persona que detectó la vulneración.
5) Llenado del formato DSB (Anexo 2), por parte de la Unidad de Transparencia del CENDI del municipio de Tlajomulco de Zúñiga.
6) Determinación de la magnitud de la afectación y elaboración de recomendaciones para las y los titulares.
7) Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia.
8) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.
9) Llenado de la bitácora de vulneraciones conforme al artículo 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD:

El CENDI Tlajomulco, por conducto de la o el titular de la unidad de transparencia, deberá realizar un informe semestral respecto al monitoreo y revisión de las medidas de seguridad, en los siguientes términos:

Primer monitoreo y evaluación de los sistemas de seguridad de cada una de las áreas que recaben o traten datos personales durante el mes de junio y presentación de informe al comité de transparencia durante los primeros diez días de julio.

Segundo monitoreo y evaluación de los sistemas de seguridad durante el mes de diciembre y presentación de informe al comité de transparencia durante los primeros diez días de enero.

PLAN DE TRABAJO

Como parte dela gestión de protección de datos personales, se ha planteado implementar la totalidad de las medidas de seguridad faltantes en un periodo de doce meses a partir de la aprobación del presente documento de seguridad y deberá estarse a lo siguiente:

Consideraciones previas a la implementación del plan de Trabajo:

El comité de Transparencia, por conducto de su Presidenta, emitirá una circular para difundir la emisión del presente documento, asimismo se realizará una sesión informativa para el personal de CENDI Tlajomulco en donde se darán a conocer las partes del presente documento, con la finalidad de esclarecer dudas y fijar los términos y plazos para su implementación.

MEDIDAS A ADOPTAR:

2) Se deben prevenir las oportunidades de fuga de información.
3) Deberán establecerse acuerdos de intercambio de información y aplicarse en este organismo y entidades externas.
4) Adopción de medidas de seguridad, tomando en consideración en análisis de riesgo y el diagnóstico realizado en cada una de las áreas.
5) Revisión y contenido del índice de datos personales y actualización del mismo.
6) Actualización del plan de trabajo en función a las necesidades supervinientes.
7) Gestión de reubicación de expedientes físicos a áreas seguras.
8) Gestión de asignación de contraseñas a los sistemas electrónicos que adolecen de ello.
9) Se deberán establecer procedimientos para monitorear el uso de la información y los sistemas, y deberán ser llevados a cabo por la o el titular de la unidad de transparencia. Los resultados de las actividades de monitoreo deben ser revisados por el comité de transparencia en los plazos establecidos en el presente documento para tal efecto.

PLAN DE CONTINGENCIA:

Clasificación de la contingencia:

Según sea el tipo de la contingencia se le pude asignar un grado de afectación:

- **Verde**: Es el tipo de contingencia con clasificación más baja; que va desde fallas eléctricas, fallas con la conexión de internet y que puede ser resuelta por el mismo personal del CENDI.

- **Amarilla**: Este tipo de contingencia requiere tanto el apoyo del personal del CENDI, así como de personal externo (Por ejemplo en un incendio apoyo de bomberos y protección civil).

- **Roja**: Este tipo de contingencia se refiere a aquella que por su alcance pueden afectar severamente la operatividad del CENDI y se requiere además del apoyo externo.

CONSIDERACIONES PREVIAS A IMPLEMENTAR EL PLAN DE CONTINGENCIA:

- Se debe realizar una evaluación de los riesgos.

- Dentro de la implementación del plan de contingencia se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.

- La o el responsable, se apoyará en las brigadas designadas por el CENDI, para que apoye en cualquier desastre que ocurra y genere la contingencia, éstos deberán contar con la debida capacitáción para el manejo de las mismas, (como el uso de extintores, planes de evacuación etc).

- Deberán realizarse pruebas previas del plan de contingencia para garantizar su funcionalidad en caso de siniestro (las pruebas generalmente se hacen en tiempo real y lo más aproximados a la realidad).

- Las brigadas deberán de recibir de manera regular la capacitación para actuar ante contingencias.

- Deberá realizarse una revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.

- Difusión del documento del plan de contingencia una vez aprobado.

MEDIDAS PREVENTIVAS ANTE SINIESTROS:

Medidas de prevención y conservación de los archivos:

- El archivo general debe ubicarse en espacios con luz natural y sin humedad.
- Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad.
- Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
- Los estantes de los archivos deben de estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita su vez la acumulación de humedad y proliferación de plagas).
- Todos los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

INCENDIOS:

- Se recomienda tener un conocimiento básico de primeros auxilios.
- Para la pronta detección de un incendio se puede contar con detectores de humo.
- En caso de incendio: no abrir puertas y ventanas, el aire es factor para propagación del fuego.
- Si se tienen almacenadas sustancias inflamables como gasolina, acetona, aguarrás, alcohol o tiner, se sugiere colocarlos en lugares ventilados y lejos de las flamas, fuentes de calor y aparatos eléctricos (si no los necesita, deséchelos preferentemente)
- Si el incendio es pequeño, se procurará apagarlo mediante un extintor. Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua.

- No sobrecargar los contactos eléctricos, desconectando los que no se utilicen.

RESGUARDO DE LA INFORMACIÓN EN CASO DE INCENDIO:

- Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es en lugares cercanos a los extintores (sugerencias para realizar el almacenamiento de la información: CD, Disco duro, bases de datos, la nube únicamente si es segura).
- Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de los mismos con resguardo en la nube).

DURANTE UN INCENDIO:

- Ubicar los extintores cerciórese de saber usarlos y que estos sean utilizables.
- Si detecta un incendio procure mantener la calma y repórtelo inmediatamente o presione alguna señal de alarma.
- No abra puertas ni ventanas el fuego se extiende con el aire.
- Si es un incendio que no puede controlar usted mismo llame a los bomberos.
- No pierda tiempo buscando objetos personales y salga del inmueble lo antes posible.
- Si hay gas o humo humedezca un trapo y cubra su nariz y boca.
- Si existe una puerta que deba atravesar toque con precaución la perilla; si está caliente no la abra.
- Si su ropa se enciende; tírese al piso y ruede lentamente.

DESPUÉS DEL INCENDIO:

Un técnico debe de revisar las instalaciones de gas y electricidad antes de utilizarlas nuevamente.

TERREMOTO:

El daño ocasionado por un terremoto puede dañar principalmente la estructura del edificio, sin embargo si los datos almacenados se encuentran en discos duros, cd, USB, al contar con un respaldo de información incluso en la nube se tiene un respaldo inmediato, que permitiría recuperar la información si los otros respaldos físicos se dañaran, para inmediatamente apenas se tenga una conexión a internet y una computadora tener acceso a dichos respaldos.

MEDIDAS PREVENTIVAS EN CASO DE SISMO:

- No colocar muebles, equipos o cajas que bloqueen las rutas y salidas de emergencia del archivo.
- Contar con un teléfono celular de emergencia en caso de falla de líneas telefónicas fijas.
- Contar con un plan de evacuación y realizar simulacros de manera cotidiana.
- Tener a la mano una radio de baterías, linterna y los principales documentos personales.
- Contar con un botiquín de primeros auxilios.
- Si se tienen anaqueles, los objetos pesados se colocan al final.
- Localizar los lugares seguros en cada cuarto; bajo mesas sólidas y escritorios resistentes
- Ubicar los lugares peligrosos: como ventanas donde los vidrios pueden estrellarse, libreros o muebles que podrían caerse en caso de sismo.

DURANTE UN SISMO:

- Mantener la calma y ubicar en una zona de segura.
- Pararse bajo un marco de puerta con trabe o de espaldas a un muro de carga.
- Adoptar posición fetal de cara al suelo, abrazándose usted mismo en un rincón, de ser posible protegerse la cabeza.
- Alejarse de ventanas, espejos y objetos de vidrio así como de objetos colgantes.
- Retirarse de objetos calientes, libreros, gabinetes, o muebles pesados.
- Si se está en un edificio evitar el uso de elevadores, si se está en la calle evitar los postes, arboles, ramas y balcones.
- Si es posible cerrar llaves del gas, desconecte la alimentación eléctrica y no encender fuego.

DESPUÉS DE UN SISMO:

- Si usted quedo atrapado, conserve la calma y trate de comunicarse al exterior golpeando un objeto.
- Evite pisar cables que hubieran quedado caídos o sueltos.
- Encienda la radio para mantenerse informado (posibles replicas).
- En caso de visible daño estructural del edificio debe ser evaluado por protección civil para evitar cualquier riesgo secundario.
- Se deben revisar las instalaciones eléctricas y de gas

principalmente para evitar un desastre secundario.

INUNDACIONES POR LLUVIA:

- Es importante realizar la revisión y reparación de la hermeticidad de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporada de lluvias esto para evitar goteras.
- Evitar en lo posible colocar expedientes y/o documentos directamente sobre el piso.
- Respetar, al menos, una altura de 10 a 15 cm de los archiveros.
- Colocar barreras para el agua (cubrir los documentos con plásticos, cubetas o recipientes para las goteras) en la parte superior de los estantes dentro del local de archivo.
- Evacuar los documentos afectados hacia áreas ventiladas.
- Inmediatamente colocar papel secante en cada hoja de los expedientes.
- Si un documento se moja en su totalidad se puede realizar la congelación del mismo para su recuperación, debe realizarlo preferentemente un especialista (restauración).

DURANTE LA INUNDACIÓN:

- Desconectar servicios de luz, gas y agua.
- Mantenerse alejados de árboles y postes de luz.
- Evitar tocar o pisar cables eléctricos.
- Cubrir con bolsas de plástico aparatos u objetos que puedan dañarse con el agua.

DESPUÉS DE LA INUNDACIÓN:

- Se puede expulsar el agua con una bomba de achique con motor de combustión o eléctrico, si hay suministro eléctrico garantizado en caso de emergencia, y si no hubiere, mediante esponjas, baldes, recogedores, etc.
- Cerciorarse de que los aparatos eléctricos estén secos antes de utilizarlos nuevamente
- Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Ventilar las áreas afectadas después de la inundación.

- Si los documentos han sufrido daños y se encuentran mojados, se debe seguir el procedimiento de congelación para recuperarlos. A continuación se describe este procedimiento para recuperar los documentos humedecidos:

1. Se introduce la obra en una bolsa de polietileno con cierre de

cremallera o termosellable. Es muy importante envolver el libro en plástico y reducir el volumen de aire para evitar la formación de condensación. Para que la congelación se realice de forma correcta, se debe dejar un amplio espacio entre los archivos.

2. La cámara de congelación debe alcanzar una temperatura de -20°C. En un proceso acelerado de descenso de la temperatura el tratamiento será más efectivo. La temperatura debe ser constante y el congelador no ha de formar hielo ya que se puede acumular humedad. Se recomienda que en el momento de Aplicación combinada de los tratamientos de congelación y vacío para la desinfección de documentos. Se debe Depositar la obra en la cámara de congelación hasta que esta haya alcanzado dicha temperatura, para evitar la aclimatación de los organismos.
3. El tratamiento debe durar como mínimo 72 horas, dependiendo del grosor de la obra y la temperatura del congelador. No obstante, si es necesario, se puede alargar hasta un periodo de tres semanas.
4. La obra se ha de descongelar de forma paulatina sin ser extraída del envoltorio, hasta alcanzar el equilibrio con la temperatura ambiente. Una vez descongelada y alcanzado el equilibrio, el envoltorio se puede retirar.

ROBO:

- En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias, así como un botón de pánico por medio de una App instalada en el celular. (https://fge.jalisco.gob.mx/content/boton-de-panico).

MANIFESTACIONES O HUELGA:

- Si el archivo tiene cerradura, asegúrese que quede bajo llave.

AMENAZA INFORMÁTICA:

Es necesario contar con un inventario actualizado de los equipos de cómputo, impresoras, escáner, fotocopiadoras etc., y tener contacto con proveedores de software, hardware, y medios de soporte.

- Prevención de falla de los equipos: se debe procurar dar mantenimiento preventivo por lo menos dos veces al año, y contar con proveedores en caso de que se requiera algún remplazo inmediato.

- Los equipos pueden quedar dañados por fallas eléctricas, se requiere contar con estabilizadores /reguladores, en cada uno de los equipos principalmente en aquellos que su afectación implique la perdida de información importante.

HACKEO INFORMÁTICO:

Ante un evento de hackeo informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:

1.- Cambiar contraseñas:

- Debe tener al menos ocho caracteres.
- No debe contener información personal como nombre real, nombre de usuario o incluso el nombre del Instituto.
- Debe ser muy distinta a tus contraseñas previas.
- No debe contener palabras completas.
- Debe contener caracteres de las cuatro categorías primarias: mayúsculas, minúsculas, números y caracteres especiales.

Mientras se está conectado a Internet el Hacker tendrá acceso a los archivos e información guardados en la computadora hackeada. Por lo que se debe **desconectar el cable de la red lo antes posible.**

Posteriormente:

- Contactar al personal de soporte para que retire del aire la página.
- Evalúe los daños causados: El experto debe evaluar qué información se perdió y cuál es la que se mantiene para restaurar el sitio lo antes posible.
- Mantener la misma dirección web: Cuando la página fue atacada la dirección usualmente no se ve afectada. Lo que generalmente se pierde es la información (textos, videos, fotos, audios) que contenía. Se sugiere restaurar el sitio con la misma dirección, para que los usuarios no se confundan.

Se sugiere cifrar documentos electrónicos.

CONTRASEÑA PARA ARCHIVO WORD:

Paso 1: **Abrir el archivo** que queramos proteger.

- Paso 2: Una vez abierto, vamos a **Archivo**. Se da clic en **Información** y le damos a
  Proteger documento, Cifrar contraseña.

  Paso 3: Acto seguido nos pide que pongamos una clave dos veces. En cuanto aceptemos, quedará registrada.

Si se desea revertir el proceso, solo deberá seguir los pasos como antes. Una vez estemos en Cifrar contraseña, simplemente tendremos que borrarla y dar clic en aceptar. Nuestro archivo de Word quedará abierto nuevamente.

También podremos hacer que nuestro documento sea sólo de lectura, restringir la edición u otorgar permisos sólo a ciertos usuarios.

CONTRASEÑA PARA ARCHIVO EXCEL:

Paso 1: Tenemos que **abrir el documento** e ir a **Archivo**, **Información**.
Paso 2: Una vez aquí dar clic en **permisos**, **proteger libro** y cifrar con contraseña.
Paso 3: Lo mismo que con el documento Word, nos pedirá una clave por dos veces. A partir de aquí nuestro archivo estará cifrado con una contraseña.

Para revertir la situación debemos de realizar el mismo proceso; borrar la clave que hemos puesto y pulsar en aceptar.

CIFRAR UN ARCHIVO:

El cifrado de archivos ayuda a proteger tus datos mediante su cifrado. Solo una persona que disponga de la clave de cifrado correcta (por ejemplo, una contraseña) puede descifrarlos. El cifrado de archivos no está disponible en Windows 10 Home.

Paso 1: Haz clic con el botón derecho en un archivo o carpeta (o mantenlo presionado) y selecciona **Propiedades**.
Paso 2: Selecciona el botón **Opciones avanzadas** y selecciona la casilla de verificación **Cifrar contenido para proteger datos**.
Paso 3. Selecciona **Aceptar** para cerrar la ventana **Atributos avanzados**, selecciona **Aplicar** y luego selecciona **Aceptar.**

CIFRAR UN ARCHIVO:

El cifrado de archivos ayuda a proteger tus datos mediante su cifrado. Solo una persona que disponga de la clave de cifrado correcta (por ejemplo, una contraseña) puede descifrarlos. El cifrado de archivos no está disponible en Windows 10 Home.

Paso 1: Haz clic con el botón derecho en un archivo o carpeta (o mantenlo presionado) y selecciona **Propiedades**.

Paso 2: Selecciona el botón **Opciones avanzadas** y selecciona la casilla de verificación **Cifrar contenido para proteger datos**.

Paso 3. Selecciona **Aceptar** para cerrar la ventana **Atributos avanzados**, selecciona **Aplicar** y luego selecciona **Aceptar.**

PROGRAMA GENERAL DE CAPACITACIÓN:

La Unidad de transparencia realizará gestiones a la Dirección de Transparencia del Municipio de Tlajomulco de Zúñiga o al ITEI para efecto de llevar a cabo la implementación de capacitación básica para las y los servidores públicos que recaban datos personales, sugiriendo las siguientes temáticas:

- Generalidad de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus municipios.
- Principios y deberes.
- Sistema de Gestión, medidas de seguridad y acciones preventivas.
- Versiones púbicas.
- Solicitudes de acceso, rectificación, cancelación u oposición de datos personales.
- Sistema de Manejo de Protección de Datos Personales.
- Seguimiento de medidas de seguridad.

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD:

REVISÓ:

Mtra. Gabriela Elizabeth Méndez González, Directora General de CENDI Tlajomulco y presidenta del Comité de Trasparencia del Centro de Estimulación para Personas con Discapacidad Intelectual del municipio de Tlajomulco de Zúñiga, Jalisco.

Lic. Jose Luis Ochoa González, Vocal de del Comité de Trasparencia del Centro de Estimulación para Personas con Discapacidad Intelectual del municipio de Tlajomulco de Zúñiga, Jalisco.

APROBÓ:

Comité de Trasparencia del Centro de Estimulación para Personas con Discapacidad Intelectual del municipio de Tlajomulco de Zúñiga, Jalisco.

Tlajomulco de Zúñiga, Jalisco a 30 de Septiembre de 2019.

ANEXO 1

FORMATO DSA.
Vulneraciones a los Sistemas de Información y Bases de Datos.

CONTENIDO DE LA BITACORA	COMPLETE EL CONTENIDO DE LA BITACORA
FECHA DEL INCIDENTE	
NOMBRE	
CARGO	
AREA	
RESPONSABLE DEL AREA	
CAUSA DE LA VULNERACION	
SISTEMA(S(DE INFORMACION O BASE(S) DE DATO(S) VULNERAD(O)	
CANTIDAD DE TITULARES	
SOPORTE DE LA INFORMACION VULNERADA	☐ Físico ☐ Electrónico ☐ Mixto
SELECCIONE EL TIPO DE VULNERACIÓN	☐ Pérdida o destrucción no autorizada ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, alteración o modificación no autorizada
TIPO DE DATOS PERSONALES COMPROMETIDOS	☐ Identificativos ☐ Laborales ☐ Tránsito y Movimientos Migratorios ☐ Académicos ☐ Procedimientos Administrativos o Judiciales Patrimoniale Salud Ideológicos ☐ De origen ☐ Características Personales ☐ Vida Sexual

Nombre y firma de quién reporta	Nombre y firma del administrador del sistema	Nombre y firma del titular del área

ANEXO 2.

FORMATO DSB.

VULNERACIONES A LOS SISTEMAS DE INFORMACIÓN Y BASES DE DATOS

CONTENIDO DE LA BITACORA	COMPLETE EL CONTENIDO DE LA BITACORA
FECHA DEL INCIDENTE	
NOMBRE DEL RESPONSABLE DE LA INVESTIGACIÓN	
CARGO	
AREA	
NÚMERO DE INVESTIGACIÓN	
LA INFORMACIÓN VULNERADA ESTA REGISTRADA EN EL DOCUMENTO DE SEGURIDAD	☐ Sí ☐ No
EN CASO DE QUE LA INFORMACIÓN NO ESTUVIERA VULNERADA, SOLICITE AL RESPONSABLE DEL ÁREA UN INFORME AL RESPECTO CON EL OBJETO DE RESPONDER EL CONTENIDO DEL APARTADO A.	
APARTADO A	
FECHA EN QUE SE CREO EL SISTEMA DE INFORMACIÓN O BASE DE DATOS VULNERADA	
FUNDAMENTO LEGAL PARA OBTENCIÓN DE LOS DATOS PERSONALES.	
RESGUARDO DE LOS SOPORTES	
USUARIOS	
MEDIDAS DE SEGURIDAD FISICAS TÉCNICAS Y ADMINISTRATIVAS APLICADAS	
LAS CAUSAS ENUNCIADAS EN EL FORMATO A	
LO QUE EL TITULAR DEL ÁREA CONSIDERE PERTINENTE	
APARTADO B	
ADMINISTRADOR DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)	
USUARIOS DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)	
LOS HECHOS DE MODO TIEMPO Y LUGAR ENUNCIADOS EN EL FORMATO A	
RESGUARDANTE SOPORTE FÍSICO O ELECTRÓNICO VULNERADO	